Remarks

In the non-final Office Action dated July 15, 2008, the following rejections are presented: claims 1, 4-5, 9-10 and 12-15 stand rejected under 35 U.S.C. § 102(b) over Satoh ("A Compact Rijndael Hardware Architecture with S-Box Optimization" (c) 2001); claims 2-3, 6-7, 11, and 16-18 stand rejected under 35 U.S.C. § 103(a) over the Satoh reference in view of Applicant's Admitted Prior Art; claim 8 stands rejected under 35 U.S.C. § 103(a) over the Satoh reference in view of Jarvinen ("A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor"). Claim 4 is objected to due to informalities. Applicant addresses these rejections in the following discussion which does not acquiesce in any regard to averments in this Office Action (unless Applicant expressly indicates otherwise).

Regarding the objection to claim 4, Applicant submits that claim 4 should be interpreted consistent with Applicant's specification, which explains that a single transform can perform affine and inverse affine functions. Applicant has amended claim 4 in this regard and requests that the objection be removed.

Applicant appreciates the Examiner's attempts to address Applicant's previous arguments. Applicant has reviewed the Examiner's response and relevant citations and submits that the Examiner's conclusions are not supported by the evidence of record.

For instance, Applicant respectfully submits that Applicant's Admitted Prior Art (AAPA) does not teach the equations or the load patterns of dependent claim 3. Accordingly, there is not a *prima facie* case of obviousness. Applicant respectfully requests that the Examiner carefully review Applicant's specification to understand the differences between AAPA and the equations and load patterns of claim 3. For instance, the Examiner is directed towards pages 4-6, which explain the differences between AAPA and the equations and load patterns consistent with claim 3 limitations. Thus, the Examiner's rejection is premised upon an assumption that is unsupported by the record. The Examiner has therefore failed to establish a *prima facie* case of obviousness.

Applicant maintains that the Satoh reference teaches implementing the inverse transformation circuit without a lookup table. The Examiner's cited portion of Satoh (page 240) explains that the S-Box has two functions, a multiplicative inverse and an affine transformation. The Examiner incorrectly assumes that the use of the term "substitution" in the context of generic S-Box functionality necessarily requires that the

inverse function be performed using a lookup table. Instead, the Satoh reference presents the following diagram for the implementation of the Examiner's alleged inverter.

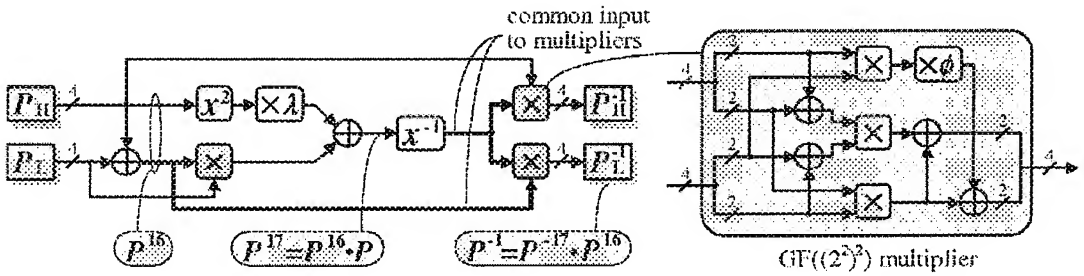


Fig. 6. Our implementation of an inverter over a composite field $GF(((2^2)^2)^2)$.

Applicant respectfully submits that this figure does not support the Examiner's assumption of a lookup table. Moreover, Satoh expressly teaches away from use of lookup tables, *e.g.*, at page 249: "(a)s a result, a large amount of hardware, 1,396 (= 696 + 700) gates, is required for each one-byte S-box based on the look-up table method, while our method is less than ¼ of that size." Thus, the record shows that Satoh disparages previous attempts that used look-up tables. Importantly, the Examiner is relying upon this allegedly improved circuit of Satoh when attempting to show correspondence to various claim limitations, and therefore, cannot use teachings from the disparaged embodiment that functions in a significantly different manner as part of an anticipation-type (§ 102) rejection. Moreover, there is no evidence that the two embodiments would function together and strong evidence teaching away for a combined use of the disparate embodiments. Accordingly, there is insufficient evidence to establish that the Satoh reference teaches each aspect of the claim limitations and there is not a *prima facie* case for the rejection.

Moreover, Applicant respectfully submits that there is not a *prima facie* case for various rejections due to a failure to address each claim limitation. For example, claim 1 includes limitations directed towards performance of both an affine and inverse affine transformation in response to respective load patterns. Claims 12 and 14 include limitations directed towards affine-all transformation with both an affine and inverse affine transformation as a single affine transformation. As another example, claims 4, 15 and 17 include limitations directed towards circuitry that performs a single transform that

accomplishes an affine and an inverse affine transformation. The Examiner has failed to present evidence that the performance of both affine transform and inverse affine transform is responsive to respective load patterns or implemented using a single affine transform. The relevant figure from Satoh is reproduced below and shows two separate and distinct transforms for each of the affine and inverse affine functions.

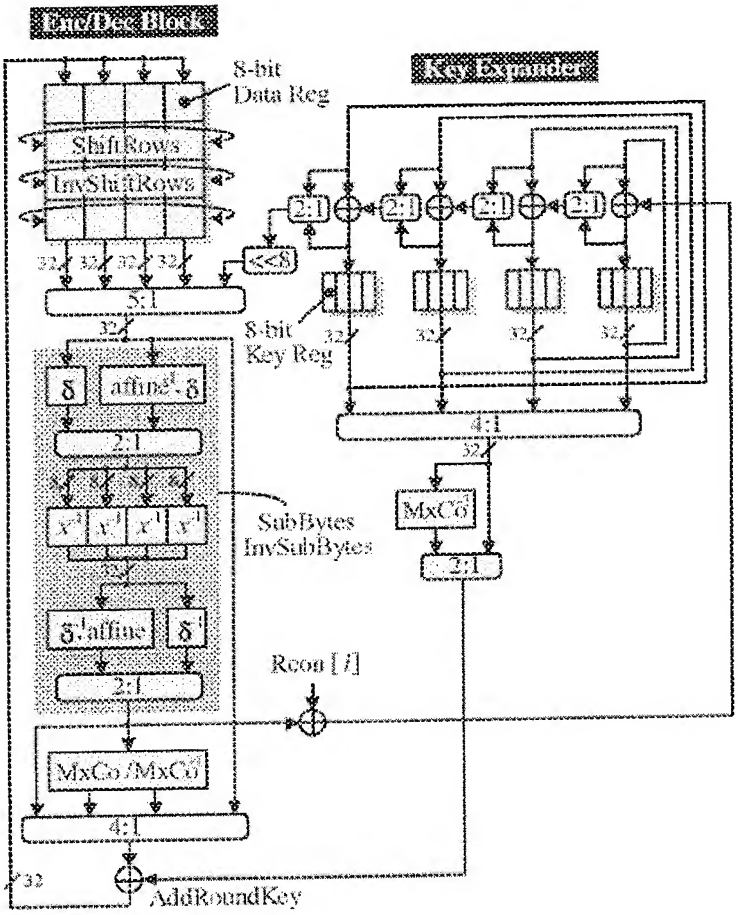


Fig. 2. Data path architecture

As should be apparent from this figure each of the affine and inverse affine transformations is implemented at a different location within the data path of the circuit. Thus, there is not a single transformation that accomplishes both affine and inverse affine transformations. This is further supported by FIG. 5 and the related discussion. Accordingly, there is insufficient evidence to establish that the Satoh reference teaches each aspect of the claim limitations. Thus, Applicant submits that none of the alleged combinations overcome the above mentioned deficiencies. Accordingly, each of the § 103 rejections is improper and should be withdrawn.

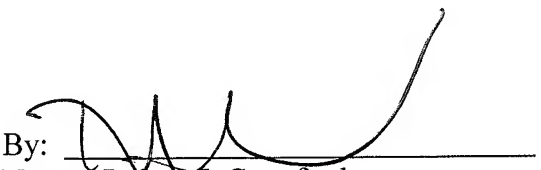
For the aforementioned reasons, the Examiner's rejection is unsupported by the cited reference(s) and therefore does not overcome the Examiner's initial burden of proof for establishing a *prima facie* case for a rejection.

In view of the remarks above, Applicant believes that each of the rejections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, Juergen Krause-Polstorff, of NXP Corporation at (408) 474-9063 (or the undersigned).

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: 
Name: Robert J. Crawford
Reg. No.: 32,122
Shane O. Sondreal
Reg. No. 60,145
651-686-6633
(NXPS.604PA)